**Guide to the Exchange Online Best Practices Checklist**

This resource corresponds to the **Office 365 Exchange Online Best Practices Checklist** and is intended to be used as a baseline for provisioning new Microsoft 365 tenants according to best practices.

© Copyright 2019-2022,

1

**Scripts to assist with configuration**

See [GitHub repository of scripts for Exchange Online.](https://github.com/vanvfields/Microsoft-365/tree/master/Exchange%20Online) will make references to these scripts throughout the guide.

**Advanced-TenantConfig.ps1**: This contains all the settings from the other scripts combined, and will allow you to customize items such as the audit log age limit, OME, Conditional Access (read-only mode), etc.

**Block**-**BasicAuth.ps1**: Creates a default authentication policy to block all forms of basic auth; see the end of the script for comments on how to make exceptions

**Block**-**ConsumerStorageOWA.ps1**: This prevents end users from using external storage locations with Outlook on the Web.

**Block-UnmanagedDownload.ps1**: Configures the Conditional Access policy option to block attachment downloads over the web. Note you must also configure a CA policy in Azure AD to complete this set up.

**Configure**-**Auditing.ps1**: Enables the Unified audit log and sets the audit log age limit

**Disable**-**Forwarding.ps1**: Disables automatic forwarding to remote domains **Disable**-**SharedMbxSignOn.ps1**: Finds and disables all shared mailboxes for sign-in **Set**-**DeletedItemsRetention.ps1**: Configures mailboxes to have maximum deleted retention period (30 days)

**Setup-DKIM.ps1**: This script helps with configuring DKIM; use: .\Setup-DKIM.ps1 -

Domain "yourdomainhere.com"

•

•

•

•

•

•

•

•

•

Deprecated scripts:

* **Baseline-Defender365.ps1**: Configures Microsoft Defender for Office 365 policies (formerly Office 365 Advanced Threat Protection)
* **Baseline-ExchangeOnline.ps1**: Configures any subscription level of an Exchange Online tenant with all the most common baseline settings and policies
* **Baseline-M365BPTenant.ps1**: Includes Baseline-ExchangeOnline.ps1 and the Baseline-

Defender365.ps1 settings in a single script

© Copyright 2019-2022,

2

**Table of Contents**

[**Guide to the Exchange Online Best Practices Checklist**](#_bookmark0)[1](#_bookmark0)

[**Items of Critical Importance**](#_bookmark1)[4](#_bookmark1)

* [**Enable the Unified Audit Log**](#_bookmark2)[4](#_bookmark2)
* [**Configure Alert policies**](#_bookmark3)[4](#_bookmark3)
* [**Block legacy (basic) authentication**](#_bookmark4)[6](#_bookmark4)
* [**Block sign-in for all shared mailboxes**](#_bookmark5)[9](#_bookmark5)

[**Items of Recommended Importance**](#_bookmark6)[10](#_bookmark6)

* [**Implement the Preset security policies**](#_bookmark7)[10](#_bookmark7)
* [**Deploy the Report Message add-in**](#_bookmark8)[11](#_bookmark8)
* [**Configure Email Authentication**](#_bookmark9)[12](#_bookmark9)
* [**Disable auto-forwarding to remote domains**](#_bookmark10)[17](#_bookmark10)
* [**Modify the default Retain deleted items value**](#_bookmark11)[19](#_bookmark11)
* [**Migrate to Microsoft 365 Groups**](#_bookmark12)[19](#_bookmark12)

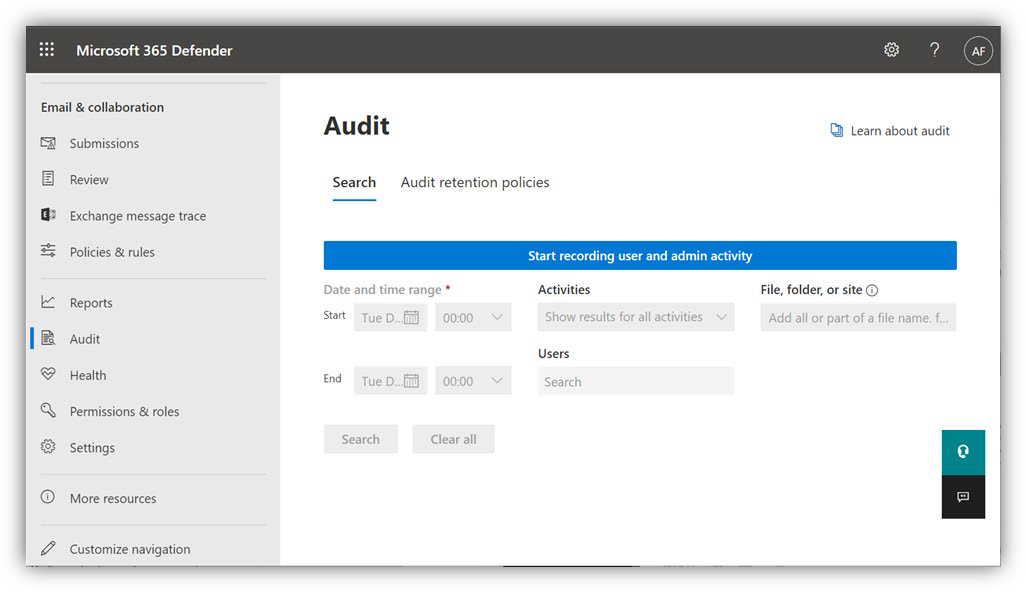
[**Items of Optional Importance**](#_bookmark13)[20](#_bookmark13)

* [**Disable consumer storage locations**](#_bookmark14)[20](#_bookmark14)
* [**Modify the default audit log age limit**](#_bookmark15)[20](#_bookmark15)
* [**Email encryption (OME) branding**](#_bookmark16)[20](#_bookmark16)
* [**Customize other settings for OME**](#_bookmark17)[21](#_bookmark17)
* [**Conditional access (Block attachment download) option**](#_bookmark18)[21](#_bookmark18)
* [**Enable auto-expanding archive**](#_bookmark19)[21](#_bookmark19)
* [**Enable the Personal Archive mailbox**](#_bookmark20)[21](#_bookmark20)
* [**Enable Litigation hold**](#_bookmark21)[22](#_bookmark21)

[**Conclusion** 23](#_bookmark22)

© Copyright 2019-2022,

3



**Items of Critical Importance**

* **Enable the Unified Audit Log**

From the [Security center](https://security.microsoft.com/) go to **Search > Audit log search** and click **Start recording user and admin activity**. Audit data is kept for 90 days by default (you can extend this timeframe but it requires additional licensing or an E5 plan).

Note that it can take several hours before the data is available for searching and alert policies. You can also achieve this by connecting to [Exchange Online with PowerShell](https://docs.microsoft.com/en-us/powershell/exchange/exchange-online/connect-to-exchange-online-powershell/mfa-connect-to-exchange-online-powershell?view=exchange-ps) and running:

Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true

Or use the scripts: **Configure-Auditing.ps1** or **Advanced-TenantConfig.ps1**.

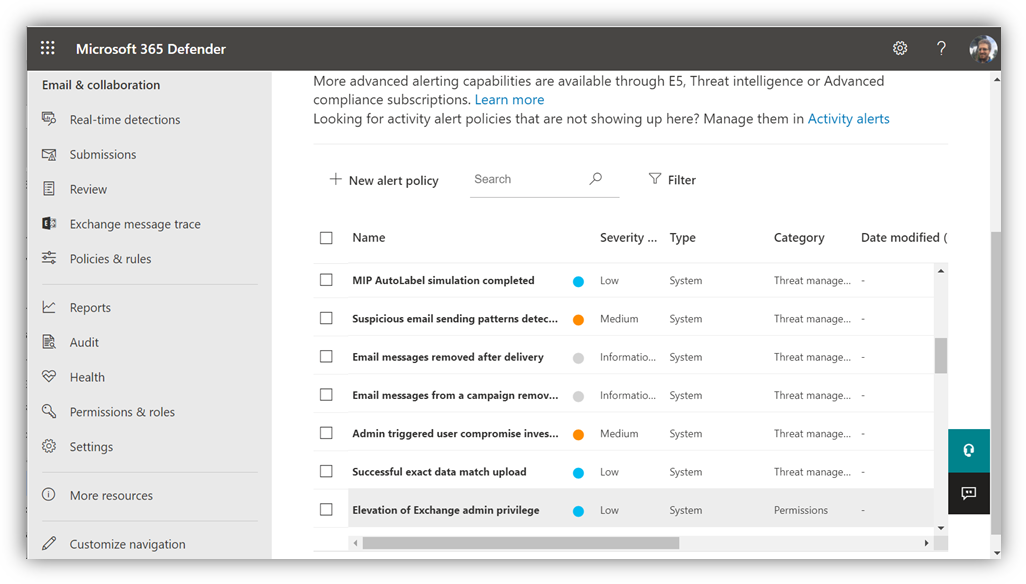
* **Configure Alert policies**

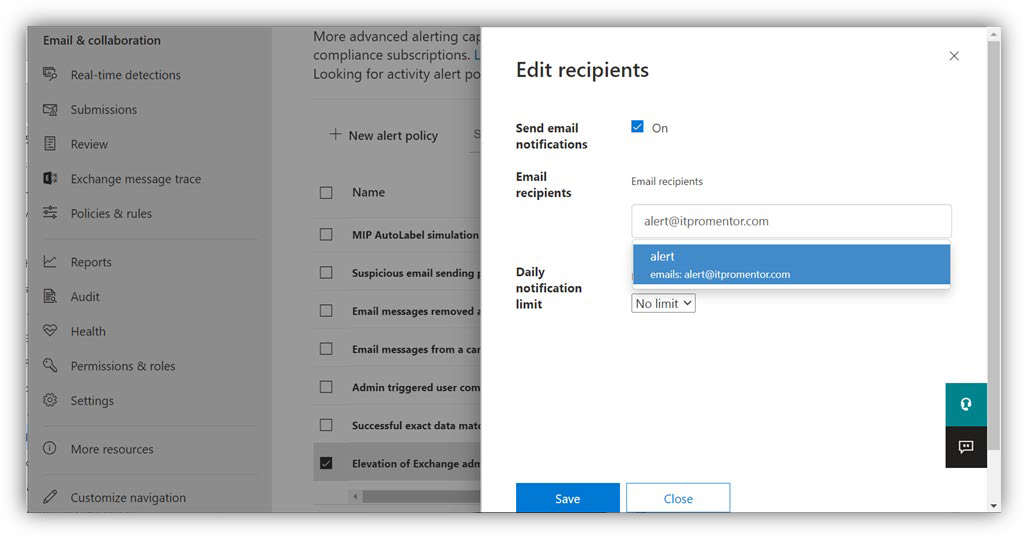
Alert Policies will generate email notifications when certain types of high-risk events happen in Office 365. From the [Security center](https://security.microsoft.com/) under **Email & collaboration** choose **Policies & rules > Alert policy**. From here, you should see at least a few basic policies which are created by

default:

© Copyright 2019-2022,

4

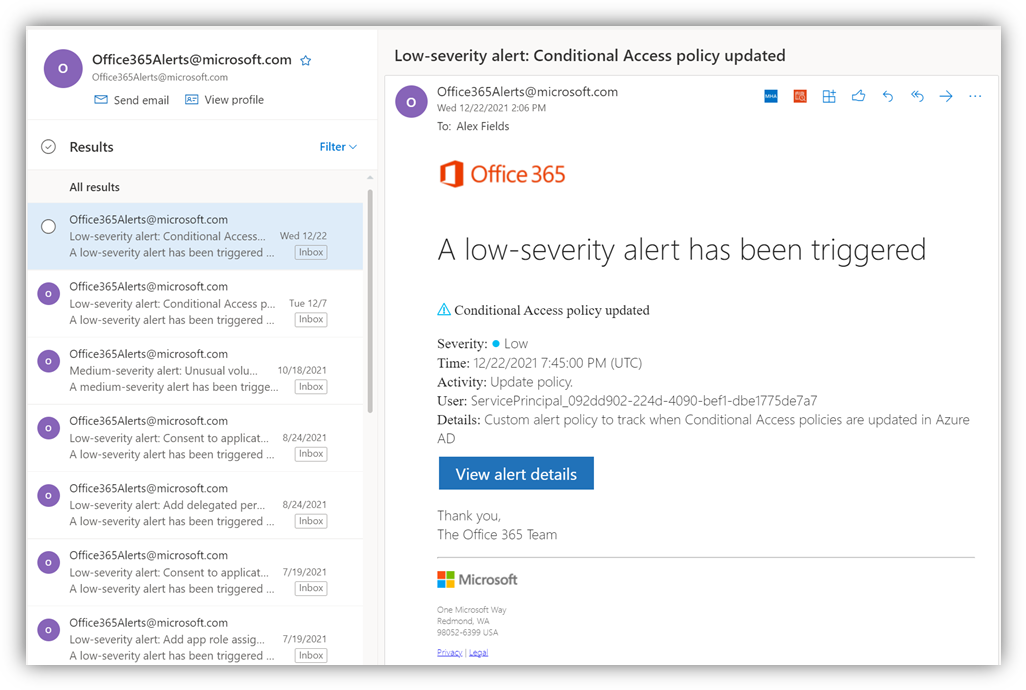




Edit the default policies now, and change the recipients to people who will actually see the alerts and be able to act on them. For example, if you are a service provider, this may be sent your ticketing system.

© Copyright 2019-2022,

5





***Note****: If you have Microsoft Defender for Office 365 plans, then this screen will include many more default (a.k.a. System) alerts.* [*Refer here*](https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies)

*for more detail on the default policies included with each subscription.*

When an alert is triggered, you can expect an email notification like the one pictured below.

The person monitoring this alert feed will need to investigate each alert and find out whether it was an expected activity, or if it was illegitimate, whether it indicates a breach or insider risk event.

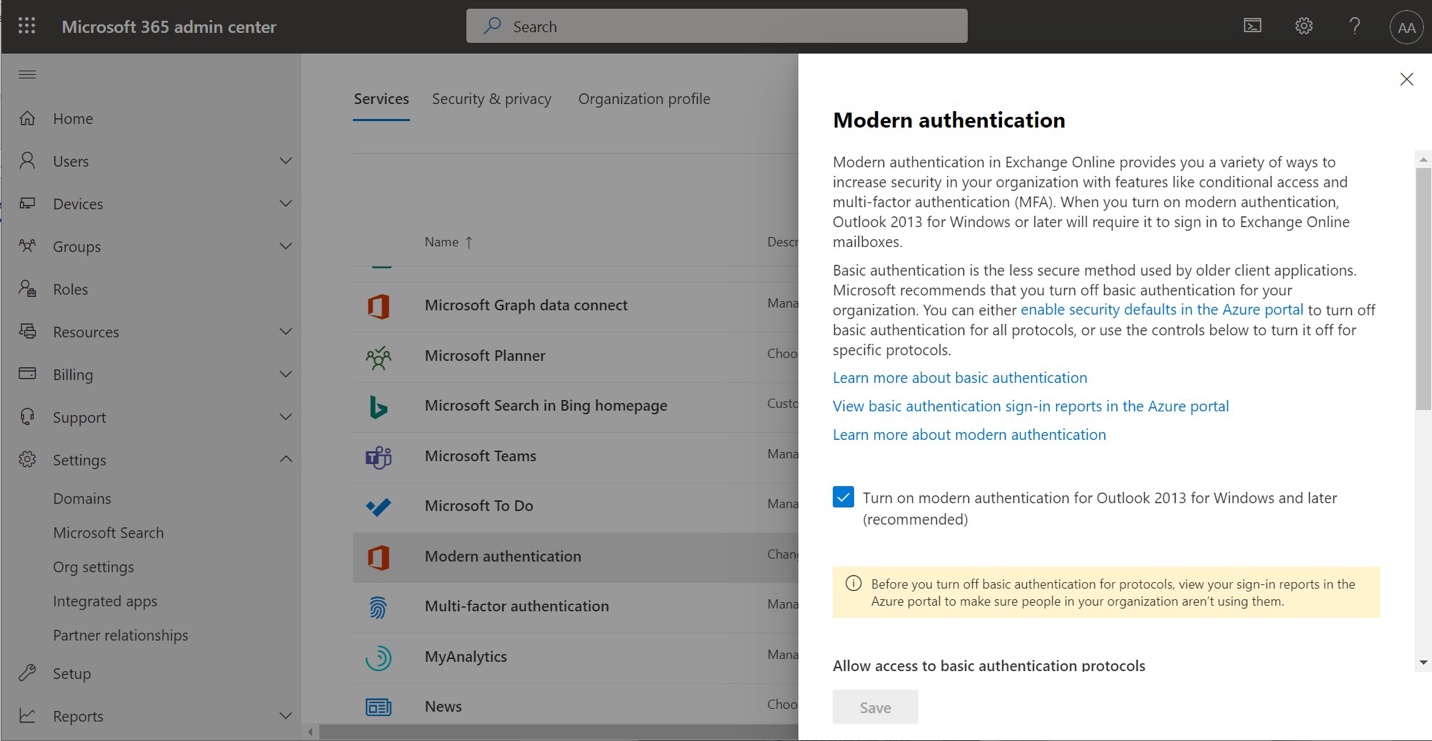
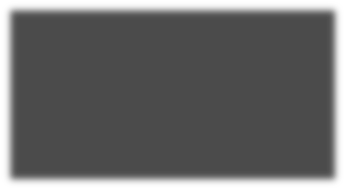
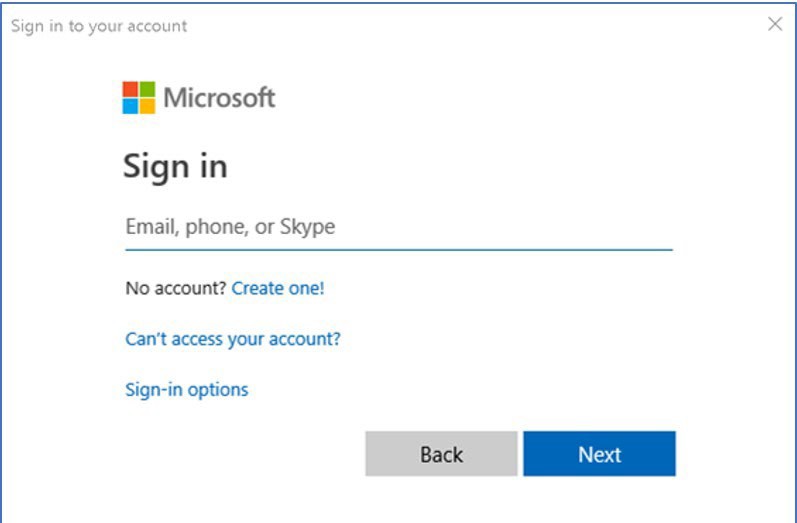
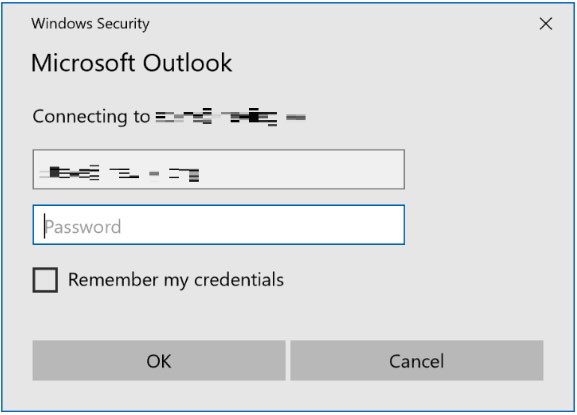
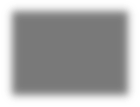
Consider configuring additional alert policies for monitoring important Azure AD activities, such as changes to Conditional Access policies and application consent requests. See [this script](https://aka.ms/aadalerts) to install several such policies that recommend.

* **Block legacy (basic) authentication**

Modern authentication is to be distinguished from legacy (or basic) authentication. Compare prompts for legacy (left) and modern (right) below on Windows client devices:

© Copyright 2019-2022,

6

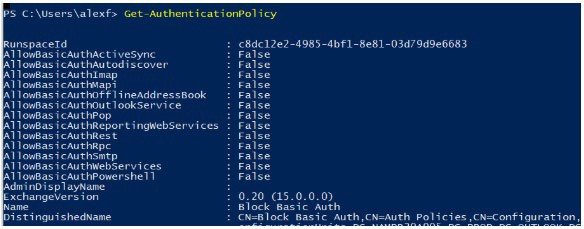


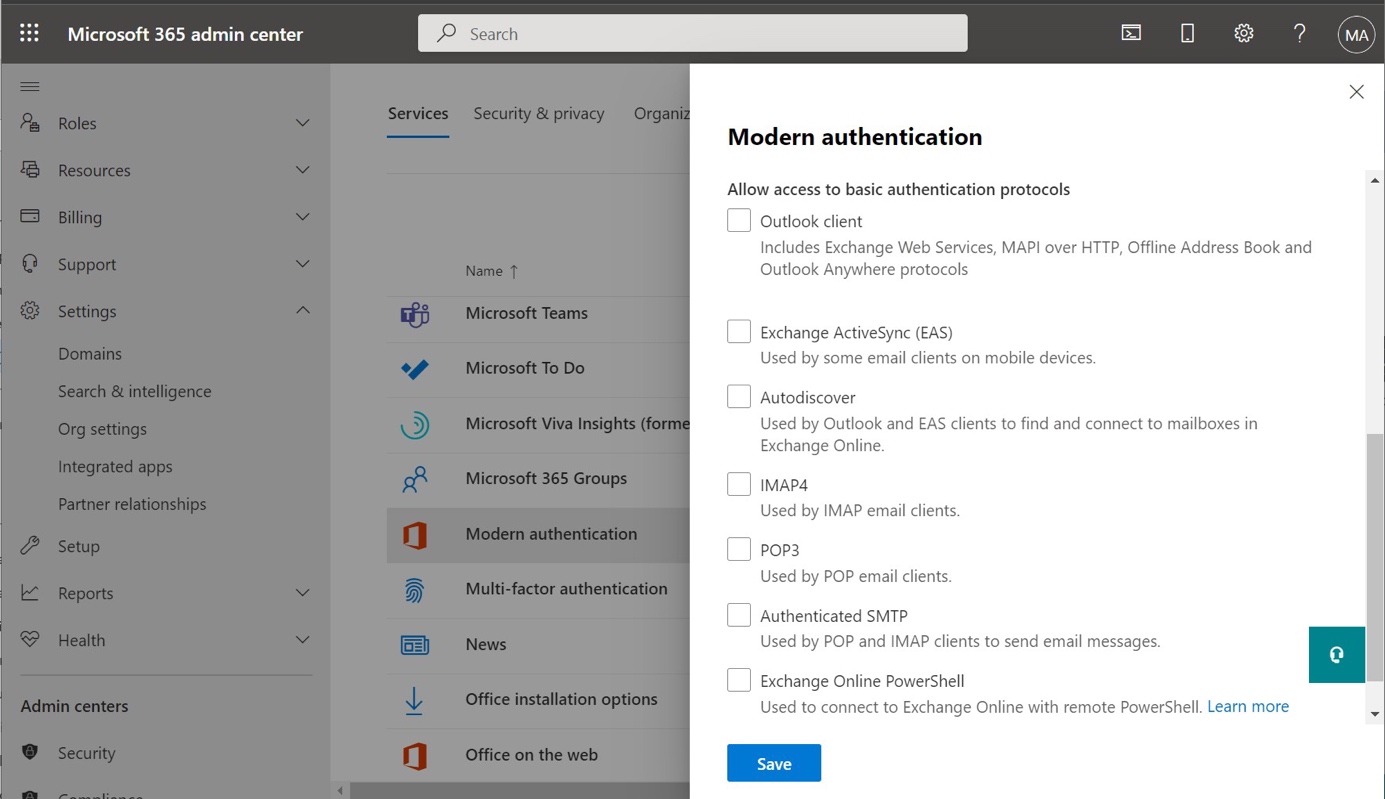
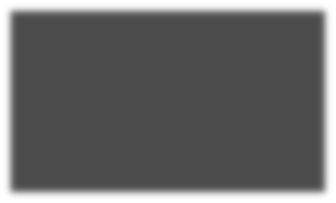
With Modern authentication clients, credentials are never stored on the device like they are with legacy clients (no option to “*Remember my credentials*”) and whenever something about the connection or state changes, the client is required to reauthenticate. This makes it less vulnerable to credential capture and replay attacks that target client devices.

Although it should be on by default, still come across older tenants where this is not yet enabled, so it is worth checking. From the admin center, go to **Settings > Org settings**, and find **Modern authentication** in the list to confirm.

© Copyright 2019-2022,

7



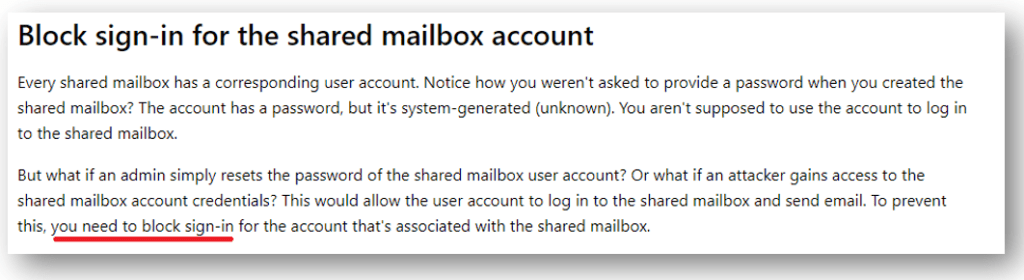


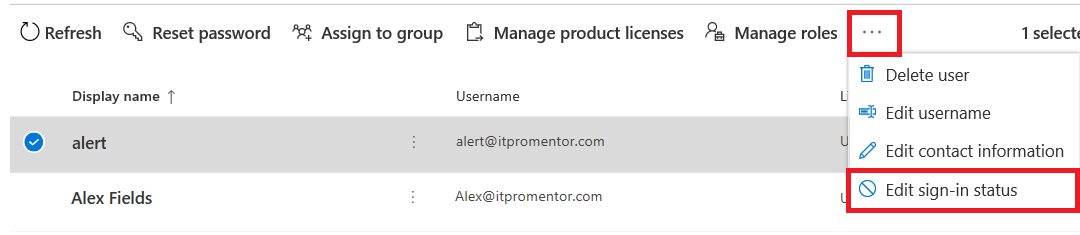
On this same page scrolling down, you have the option to allow or remove access for various legacy authentication protocols (a cleared checkmark box means the service has been *disabled* for basic auth). Switching these on or off will modify an [Authentication policy](https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online) in Exchange Online. Clear the checkboxes to disable all basic auth protocols.

*NOTE: If you want to see all authentication policies in the organization, simply run* ***Get-AuthenticationPolicy****.*

© Copyright 2019-2022,

8





See my script titled **Block-BasicAuth.ps1**, or **Advanced-TenantConfig.ps1**.

If you need to make exceptions for individual accounts, an example of making exceptions is also detailed at the end of the script—it is commented out so that it will not run by default.

Mailboxes that have a specific policy assigned will override the default policy that you set for the organization. The org-wide policy is applied only if there is no specific policy assigned to the mailbox.

* **Block sign-in for all shared mailboxes**

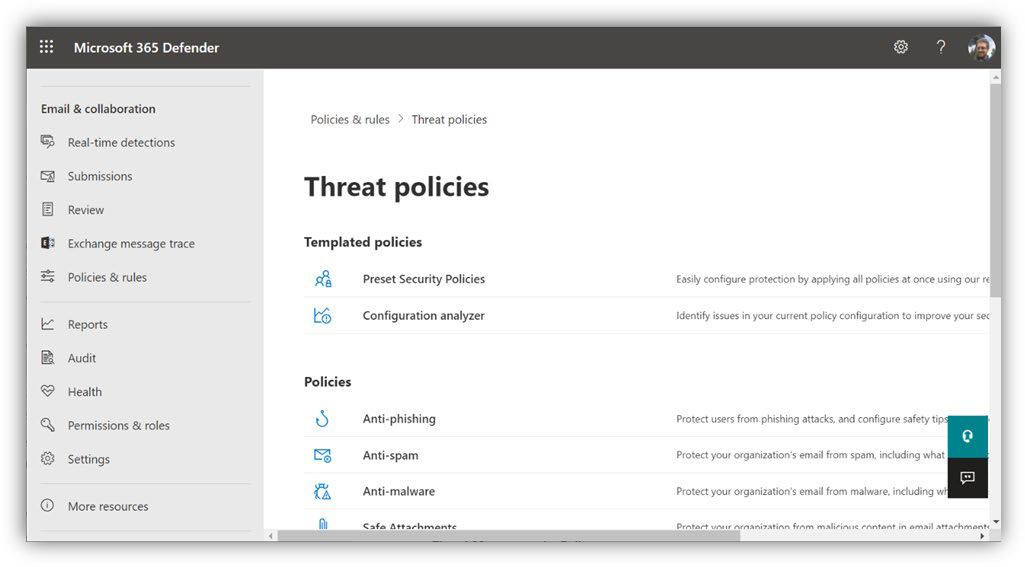
Shared mailboxes (including Resource mailboxes) should not require interactive login. Rather, users who are delegated permission can access and interact with the contents of the shared mailbox. When organizations allow multiple users to sign into shared mailboxes on mobile devices, they are not working within the conceptual framework of a shared mailbox. So effectively, those which are enabled for interactive sign-in become real user mailboxes. But hardly anyone thinks to enable these for MFA.

Really though, you should be blocking sign-in for these accounts. Note that accounts which are synced from on-premises Active Directory would need to be disabled on-premises. In the 365 admin center, select one or multiple accounts and **Edit the sign-in status** from the **ellipses**.

have a script called **Disable-SharedMbxSignOn.ps1** in the GitHub repository which will find and disable sign-in for all the shared mailboxes simultaneously. However, note that this requires

© Copyright 2019-2022,

9



the accounts to be labeled accurately as shared or resource mailboxes. It is best to audit your accounts to be positive that any “non-real-person” sign-ins are disabled.

**Items of Recommended Importance**

* **Implement the Preset security policies**

[Microsoft publishes](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365-atp?view=o365-worldwide) two sets of recommended settings for Exchange Online Protection and Microsoft Defender for Office 35: **Standard** and **Strict**. My scripts will apply settings that are consistent with the *Standard* protection profile.

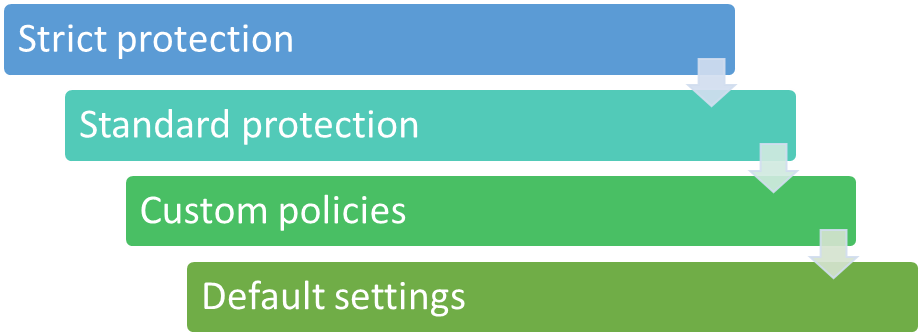
However, Microsoft now presents us with the “easy button” in the Security center allowing you to apply the “**Standard protection**” as well as the “**Strict protection**” template to your tenant. This is the preferred way to apply the recommended settings because they will be automatically updated when something about the service changes.

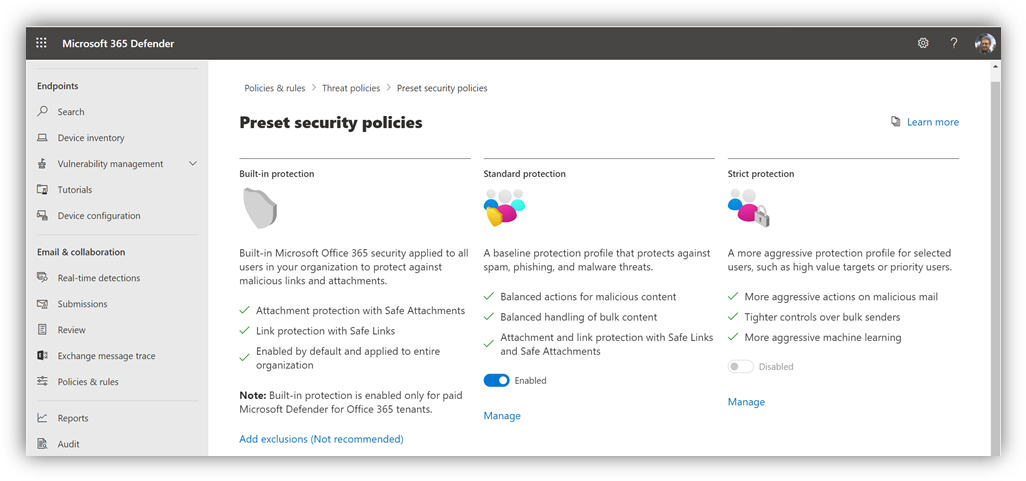
In the [**Security center**](https://security.microsoft.com/)under **Policies & rules**, find **Threat policies > Preset Security Policies**.

While it is still possible to manage all of your individual policies separately of course, still recommend most small and mid-sized customers stick with the *Presets*. Especially because Microsoft may update their best practices over time. With the presets in place, you will be automatically upgraded when Microsoft adds or removes features, or alters settings based on threats that Microsoft is seeing in the wild. If you do decide to manage custom policies yourself, then please refer to [this Microsoft Docs article](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide) for guidance (and revisit on a regular cadence).

© Copyright 2019-2022,

10





***Note****: find that the ‘Strict protection’ leads to more false positives, while ‘Standard protection’ works well for most organizations.*

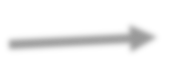
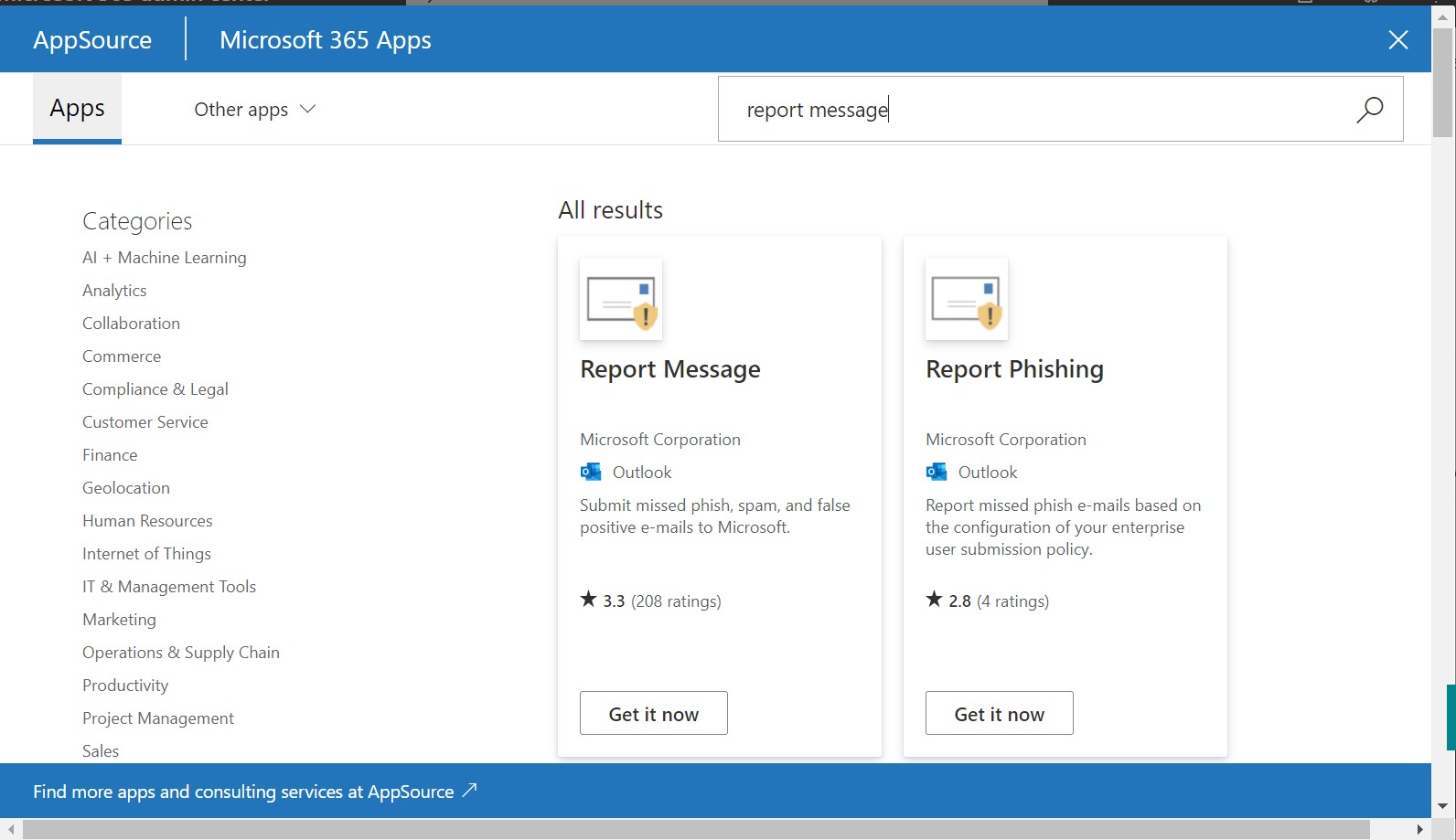
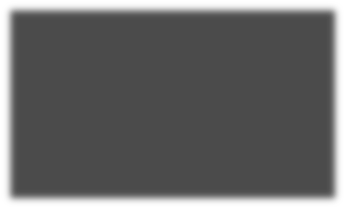
Regarding policy precedence: **Strict** overrides **Standard** overrides **Custom** overrides **Default**. So, what does that mean? It means if you deploy a **Preset** policy, it will take precedence over any custom or default policies you have out there. Remember that **Strict** will always outstrip **Standard**; so, if a user falls under the scope of two policies, now you know which one wins.

* **Deploy the Report Message add-in**

Not every bad thing will be caught by your security policies; some items might slip by. Therefore, you should give end users the ability to self-report email messages that they believe are junk or phishing, by providing them with the **Report Message** add-in.

© Copyright 2019-2022,

11



From the [Admin center,](https://admin.microsoft.com/) go to **Settings > Integrated apps** and click **Get apps**. From the store, you can find the **Report Message** add-in here and click **Get it now**.

Finish the wizard to deploy this add-in for all users, but note that it can take up to 12 hours to appear in Outlook.

* **Configure Email Authentication**

Email authentication is a means of using DNS records to validate or prove that your email is coming from a trusted source. Therefore, it is important that you also protect access to your DNS hosting provider, where these changes can be made. There are three record types in total that we need to configure.

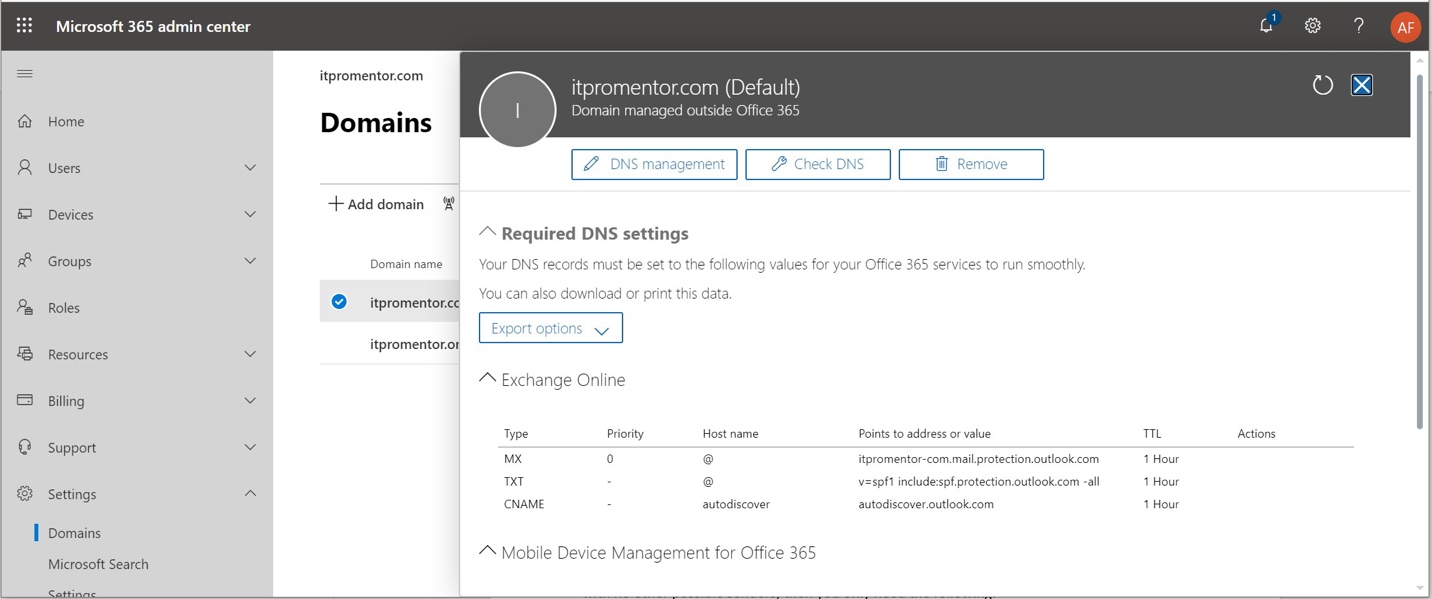
**Sender Policy Framework (SPF)**

An [SPF record](https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-spf-in-office-365-to-help-prevent-spoofing) is a DNS “TXT” type record. It is one of the records that Office 365 has you provision when you first setup and configure mail flow to Office 365. Navigate in the Microsoft 365 admin center to **Settings > Domains**.

© Copyright 2019-2022,

12

Just search for “report message” to filter the list



The function of the SPF record is to advertise to the world who is allowed to send email on behalf of your domain. When you build this TXT record, you should try to include as many “legitimate” sources of email as you can. For example, for email that is hosted at Office 365, with no other possible senders, then you only need the following:

For third-party software such as Mail Chimp, Constant Contact, etc., you can usually find their SPF information using a quick Google search, or by contacting their support. For your own on- premises apps or scan to email devices, you may want to include an ip4 entry for your company’s external IP addresses.

Let us assume you had a combination of Office 365 for hosted email, Constant Contact for bulk mailing/marketing emails, and an on-premises copier/scanner internally, with your organization’s external IP being 87.65.43.21. Then you would have this SPF to publish:

**Domain Keys Identified Mail (DKIM)**

[DKIM](https://docs.microsoft.com/en-us/office365/securitycompliance/use-dkim-to-validate-outbound-email) is an authentication system based on an asymmetric cryptographic key pair–a private and

© Copyright 2019-2022,

13

Host name: @ <or your domain name> TXT value:

v=spf1 include:spf.protection.outlook.com include:spf.constantcontact.com ip4:87.65.43.21 -all

Host name: @ <or your domain name>

TXT value: v=spf1 include:spf.protection.outlook.com -all

public key. When a message leaves Office 365, it is digitally signed with the private key. The public key is published via a DNS CNAME record, so that recipient servers can validate the signature. This proves to recipient servers that your messages really did come from the “right place.”

By default, your “OnMicrosoft” domain already has DKIM configured and working. But if you are bringing a “vanity” domain name such as contoso.com (most organizations are), then you will need to setup DNS records for your domain(s), and then enable DKIM message signing in Exchange Online.

You will need to build two CNAME records per domain for DKIM. The format is:

*Note: Your domain is separated by a hyphen instead of a period; it should match the domain as depicted in the MX record that is given to you by Office 365*

*(e.g.:* ***contoso-com****.mail.protection.outlook.com).*

*Also, the tenant name (****TenantName****.onmicrosoft.com) can be found under*

***Settings > Domains*** *in the Microsoft 365 admin center.*

Therefore, contoso.com, whose tenant name is “contoso.onmicrosoft.com” looks like this:

Another example is myfavoritecharity.org with a tenant name of charityrocks.onmicrosoft.com:

© Copyright 2019-2022,

14

**Host name**: selector1.\_domainkey

**Points to**: selector1-**myfavoritecharity-org**.\_domainkey.**charityrocks**.onmicrosoft.com

**Host name**: selector1.\_domainkey

**Points to**: selector1-**contoso-com**.\_domainkey.**contoso**.onmicrosoft.com

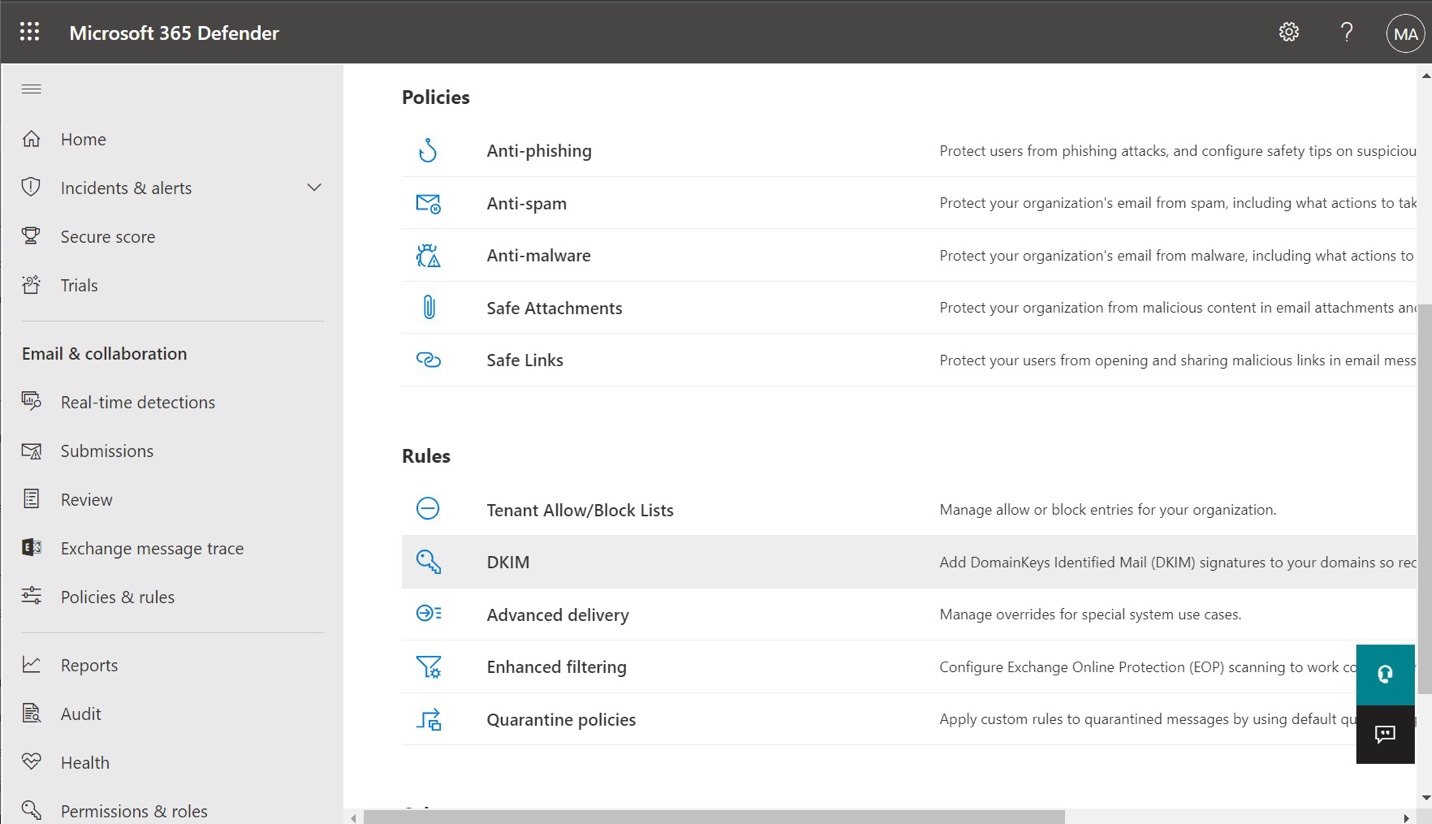
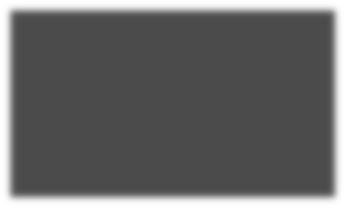
**Host name**: selector2.\_domainkey

**Points to**: selector2-**contoso-com**.\_domainkey.**contoso**.onmicrosoft.com

Host name: selector1.\_domainkey

Points to: selector1-**CompanyDomainName-com**.\_domainkey.**TenantName**.onmicrosoft.com Host name: selector2.\_domainkey

Points to: selector2-**CompanyDomainName-com**.\_domainkey.**TenantName**.onmicrosoft.com



Next, in the **Security admin center**, go to **Policies & rules > Threat Policies** and scroll down under **Rules** to find **DKIM**. Pick the domain that you want to enable for DKIM signing.

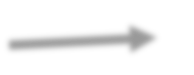
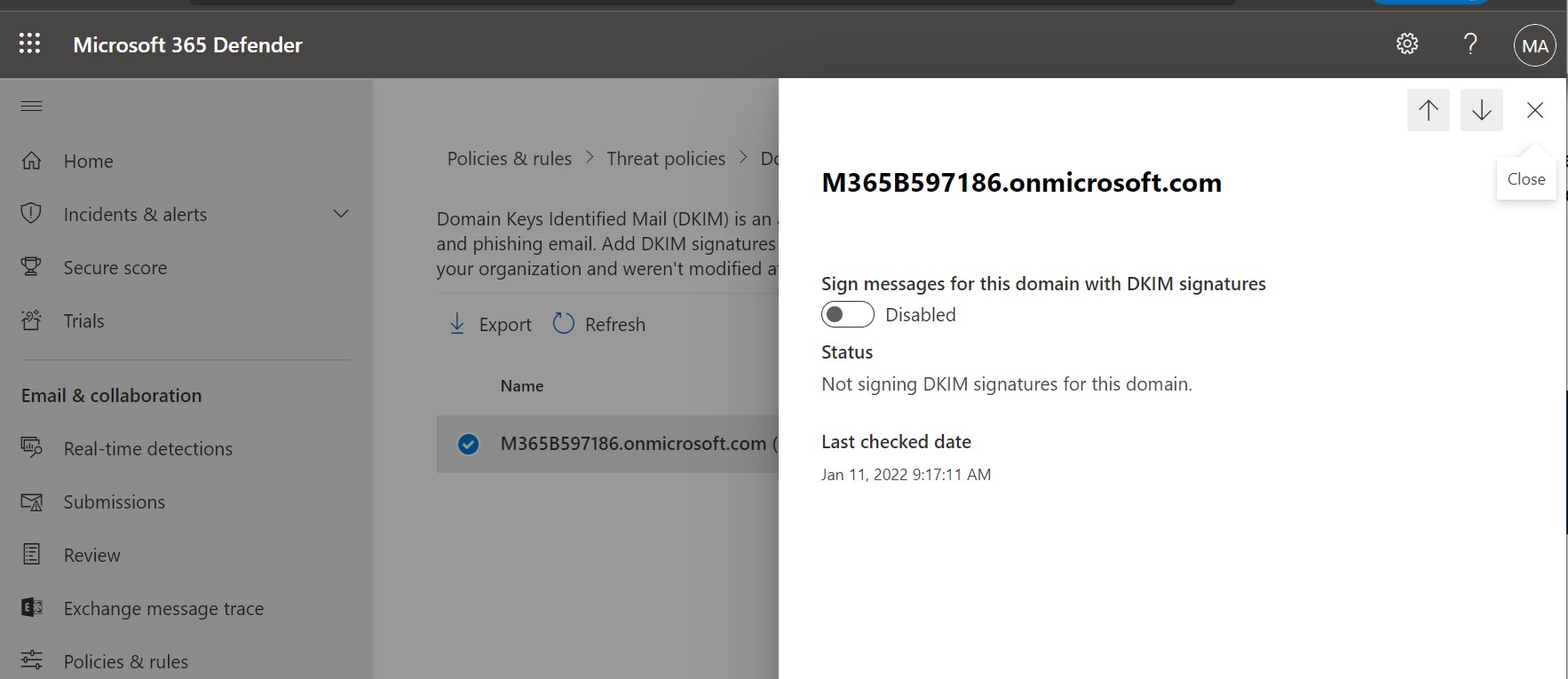
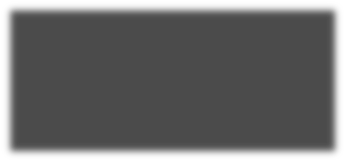
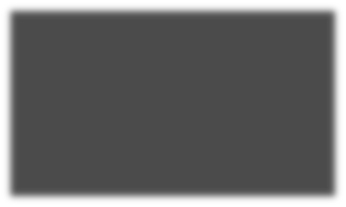
In the right-hand flyout that appears, you can generate your DKIM keys for the selected domain; you must publish these records via your DNS hosting provider.

© Copyright 2019-2022,

15

**Host name**: selector2.\_domainkey

**Points to**: selector2- **myfavoritecharity-org**.\_domainkey.**charityrocks**.onmicrosoft.com



Give it at least a few minutes after publishing before you attempt to **Enable** signing. If you have not configured your DNS records, this operation will fail out, so be sure to allow enough time for DNS to propagate.

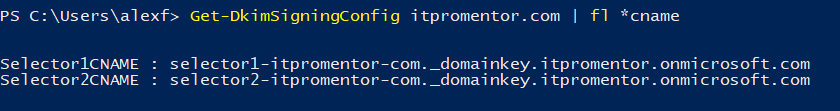
After DNS changes

are made, then

**Enable** here

© Copyright 2019-2022,

16



You may also see the script entitled **Setup-DKIM.ps1** in my [GitHub repo](https://github.com/vanvfields/Microsoft-365) for a quick way to retrieve the “points to” values.

***NOTE****: You should also work with third-party authorized senders get their DKIM information and enable signing as well.*

**Domain-based Message Authentication, Reporting & Conformance (DMARC)** [DMARC](https://docs.microsoft.com/en-us/office365/securitycompliance/use-dmarc-to-validate-email) is a DNS record that tells recipient servers how to treat unauthenticated messages that come from your domain, based on policy. It can also communicate where to send reports about mail from your domain.

By way of example, here is what DMARC could look like for **contoso.com**:

However, when you are first rolling DMARC out, it is best to start with the policy set

to **p=none**, because this will allow you to take time to find legitimate sources of email and update SPF and DKIM *before* moving the DMARC policy up to a setting of **quarantine**, or even **reject** (the strongest setting).

* **Disable auto-forwarding to remote domains**

When attackers get a hold of a mailbox, they will often exfiltrate data by setting up mailbox forwarding to an outside email address that they can then monitor without needing constant access to the source mailbox. In fact, one of the default Alert policies that we enabled in step 2 will notify you when new rules like this show up.

There are two things would recommend that you do to defend against this:

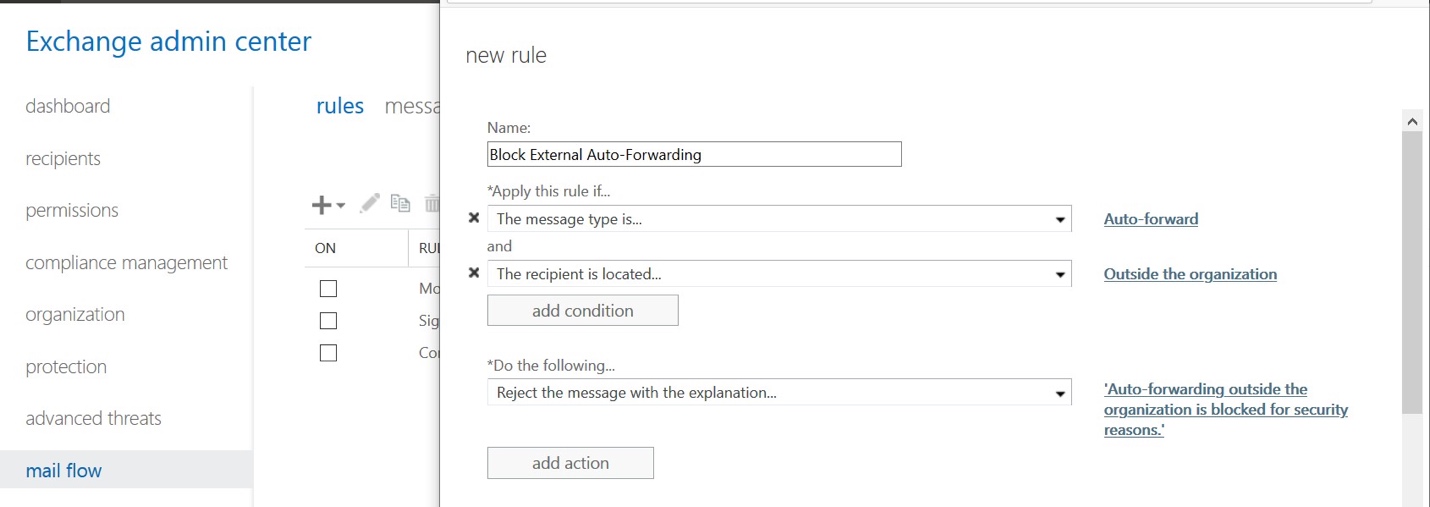
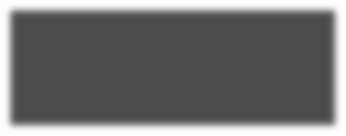
* + Create a transport rule that will reject auto-forwarded messages with a notification
  + Disable the auto-forward capability globally

© Copyright 2019-2022,

17

TXT Name: \_dmarc.**contoso.com**

Value: "v=DMARC1; p=quarantine; pct=100”



The **Disable-Forwarding.ps1** script or the **Advanced-TenantConfig.ps1 script** will accomplish both for you quickly. To manually create a transport rule in the web portal, go to the **Exchange Admin Center**.

* Under **mail flow**, select **rules**.
* Select **+**, and then **Create a new rule**.
* Select **More options** at the bottom of the dialog box to see the full set of options.
* Apply the settings in the following table.
* Select **Save**.

Next, in the Exchange admin center also under **mail flow > remote domains**. Edit the **Default**

remote domain object **(\*).**

© Copyright 2019-2022,

18

**Setting**

**Prevent auto forwarding of email**

Name

Block External Auto-Forwarding

Apply this rule if ...

The message properties . . . include the message type . . . Auto-forward

Add condition

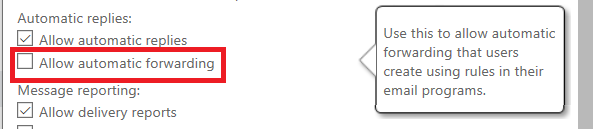
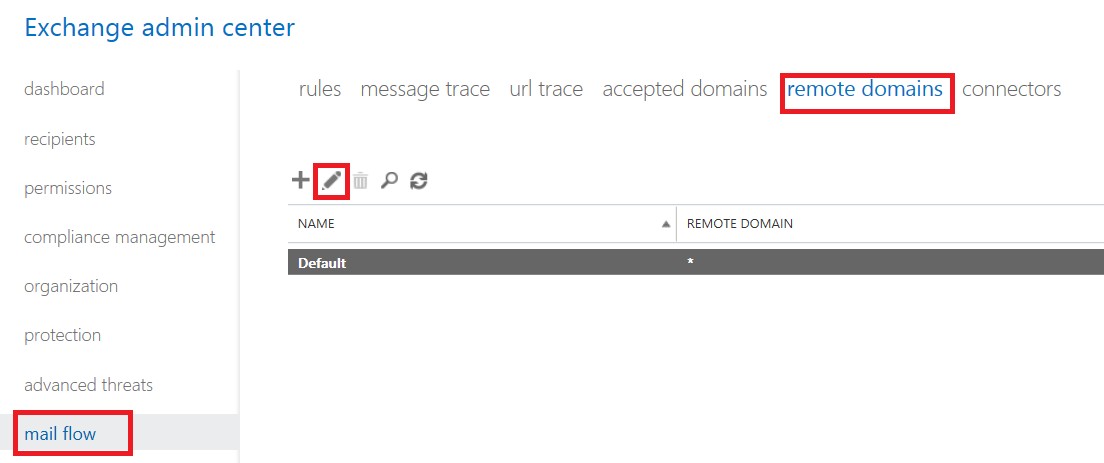
The recipient . . . is external/internal . . . outside the organization

Do the following ...

Block the message . . . reject the message and include an explanation.

Provide message text

Auto-forwarding outside the organization is blocked for security reasons.



Clear the selection for **Allow automatic forwarding**.

To enable exceptions, you would create a new remote domain (to a specific place like a partner organization) and then enable the option instead of disabling it.

* **Modify the default Retain deleted items value**

By default, deleted items will be purged after 14 days, but this is extendable to 30 days. We can set on all mailboxes individually (existing mailboxes) and the mailbox plan (for future mailboxes). See the **Set-DeletedItemsRetention.ps1** script; it is also included with **Advanced- TenantConfig.ps1**.

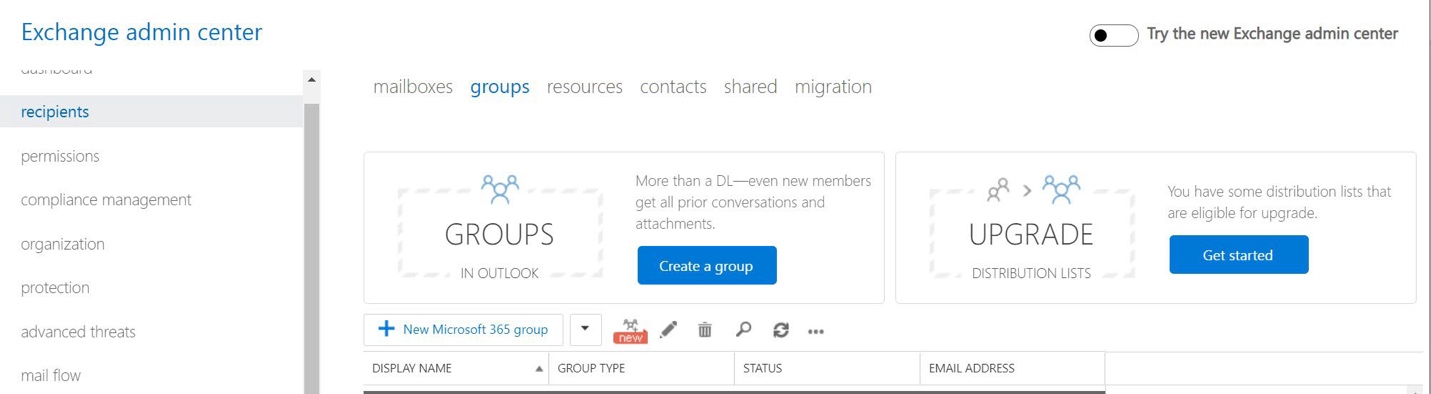
* **Migrate to Microsoft 365 Groups**

Many organizations have legacy Distribution Lists and Public Folders which could be replaced with Microsoft 365 Groups. It is recommended to look for opportunities to leverage Groups

where it makes sense. In fact, many times a business process that relied on Public Folders or

© Copyright 2019-2022,

19



Distribution Lists in the past would make much more sense in an altogether different application like Teams! (And remember that Teams is built on top of Microsoft 365 Groups).

Microsoft provides a mechanism to upgrade Distribution Lists, but the same does not exist for Public Folders. Most of the time this process ends up being a manual review and replace, but for more information on how to upgrade DL’s at least, you can refer to this article:

<https://docs.microsoft.com/en-us/microsoft-365/admin/manage/upgrade-distribution-lists>

**Items of Optional Importance**

* **Disable consumer storage locations**

By default, users can work with consumer storage locations such as DropBox, Gsuite and OneDrive (personal) via Outlook on the Web. In some environments, this will be exposing the organization to unnecessary risk—consumer storage locations are unmanaged and outside of the compliance boundary of Microsoft 365.

See **Block-ConsumerStorage.ps1**; this is also available in **Advanced-TenantConfig.ps1**.

* **Modify the default audit log age limit**

By default, the audit log age limit is 90 days. If you have an E5 subscription, you can adjust this value using **Configure-Auditing.ps1**, or **Advanced-TenantConfig.ps1**, e.g.:

$AuditLogAgeLimit = 365

Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditEnabled

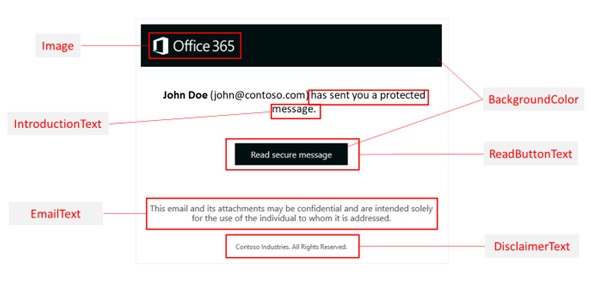
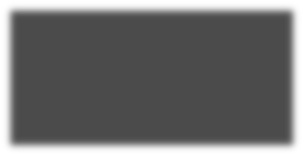
$true -AuditLogAgeLimit $AuditLogAgeLimit

* **Email encryption (OME) branding**

It is possible to configure custom branding elements for Office 365 Message Encryption (OME).

© Copyright 2019-2022,

20



See [this article](https://docs.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to-encrypted-messages?view=o365-worldwide&modify-an-ome-branding-template) for more details.

* **Customize other settings for OME**

See my **Advanced-TenantConfig.ps1** script for quick modifications including:

•

•

•

Encrypt PDF attachments (they are not encrypted by default)

Auto decryption for copies of messages sent to third-party journal providers Auto decryption for download of attachments on OME protected messages

* **Conditional access (Block attachment download) option**

In order to enable app enforced restrictions, you must first enable the Conditional Access policy in Read-only mode via PowerShell. See my script titled **Block-UnmanagedDownload.ps1** (also included with **Advanced-TenantConfig.ps1**). It is necessary to subsequently set up a Conditional Access policy in Azure AD. See [this blog](https://techcommunity.microsoft.com/t5/outlook-blog/conditional-access-in-outlook-on-the-web-for-exchange-online/ba-p/267069) and my Conditional Access guide for more details. This is recommended in sensitive environments where compliance and data leakage are major concerns.

* **Enable auto-expanding archive**

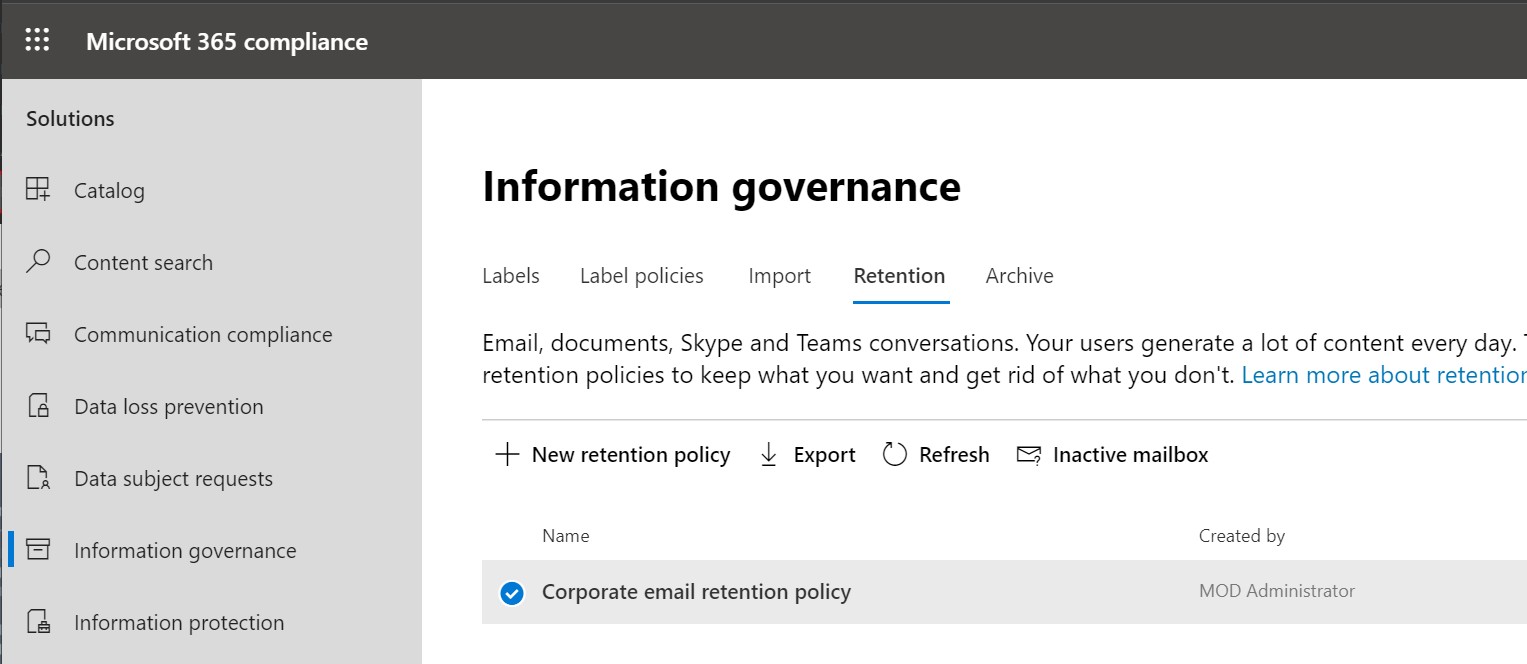
The archive mailbox can be automatically expanded when it reaches its capacity. At the time of this writing, it will continue to auto-expand up to a maximum limit of 1 TB. See either script: **Setup-ArchiveLegalHold.ps1** or **Advanced-TenantConfig.ps1**.

* **Enable the Personal Archive mailbox**

See either script: **Setup-ArchiveLegalHold.ps1** or **Advanced-TenantConfig.ps1** to enable the archive mailbox. This is simply another mailbox that can be used to store old items, and act as

© Copyright 2019-2022,

21



additional storage space which will relieve pressure on the storage quotas that you have by default on the primary mailbox.

* **Enable Litigation hold**

See either script: **Setup-ArchiveLegalHold.ps1** or **Advanced-TenantConfig.ps1** to enable the litigation hold feature across all mailboxes. The only reason you would do this with no expiration date defined is if the customer wants to preserve 100% of email data. However, be aware that keeping too much data can be a risk as well for some organizations. It is also possible to manage retention (as well as deletion) using Retention policies in the Compliance admin center. See the **Microsoft 365 SMB Data Protection Toolkit** for more information.

**Inactive mailboxes**

Once you have a mailbox on hold or you have applied a general retention policy to Exchange Online, then you also enable **Inactive mailboxes**—these are just deleted mailboxes that are still available for recovery, throughout the period of the hold or retention.

Find the Inactive mailboxes in the traditional Security & Compliance center, or the new Microsoft 365 Compliance center, under **Information Governance > Retention**.

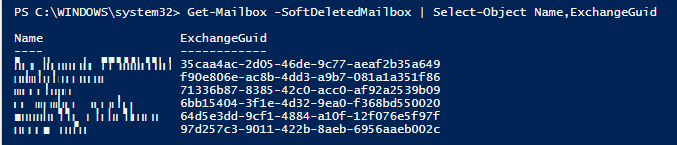
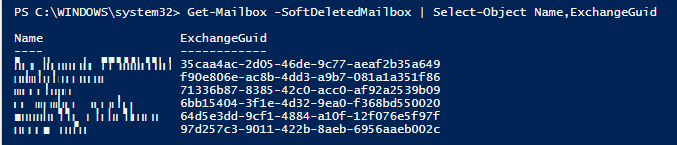
Or view them via PowerShell:

Get-Mailbox -SoftDeletedMailbox | Select-Object Name,ExchangeGuid

© Copyright 2019-2022,

22

See the **Inactive mailboxes**



When an employee leaves the company, they are typically replaced by a new hire. But when we remove licenses from user accounts in Microsoft 365, the mailbox is also removed. While it is possible to recover on short time horizons (e.g. 30 days), retention policies and legal holds will ensure that mailboxes remain recoverable for the duration of the preservation period. Therefore, mailboxes become “inactive” rather than deleted.

Microsoft supports two methods for pulling these mailboxes back from the grave:

1. [Recover the inactive mailbox](https://docs.microsoft.com/en-us/office365/securitycompliance/recover-an-inactive-mailbox) (e.g. if the departed user returns to the organization) or
2. [Restore the inactive mailbox](https://docs.microsoft.com/en-us/office365/securitycompliance/restore-an-inactive-mailbox) to an alternate location (merge it into another mailbox)

© Copyright 2019-2022,

23